Safety and Verification for a Mobile Guide Robot

Jonathan M. Aitken, Owen McAree, Luke Boorman, David Cameron, Adriel Chua, Emily C. Collins, Samuel Fernando, James Law, Uriel Martinez-Hernandez

Sheffield Robotics, University of Sheffield,
Pam Liversidge Building, Sheffield,
South Yorkshire, S1 3JD, United Kingdom
{jonathan.aitken,o.mcaree,l.boorman,d.s.cameron,
dxachua1,e.c.collins,s.fernando,j.law,
uriel.martinez}@sheffield.ac.uk

Abstract. This work presents the safety and verification arguments for the development of an autonomous robot platform capable of leading humans around a building. This paper develops a pattern that can be used in the safety case surrounding the positioning of the robot using Goal Structured Notation to: record the decisions taken during the design phase, ensure safe operation around humans, and identify where mitigation must be introduced. This ensures a coherent argument about the safety of such a robot.

1 Introduction

As the robotic technology improves and the capability of robots increases, they will become a more common-place occurrence in daily life. This will them into direct contact with humans not accustomed to autonomous robots in their daily life. Appropriate design and implementation will be required to increase awareness and to ensure good engineering takes place so that technology is implemented safely.

This paper discusses the safety concerns of deploying an autonomous robot, ROBO-GUIDE [1], that is able to navigate corridors of a building and acquire human help in using a lift to reach different floors [3]. In undertaking this task the robot will come into regular contact with people, and have to co-exist in an everyday environment whilst maintaining autonomy. This requires an analyses of the operational safety to be performed, to ensure that potential hazards are identified and dealt with appropriately.

Formal verification is proposed as a method for ensuring the decisions made by the robot will always be safe. To achieve this, a set of specifications are required which describe the safe operation of the robot and also its desired performance. Performance must be considered during verification to ensure that safety is not achieved only at the expense of goal achievement. These specifications rely

on abstractions about the environment [4] which can initially be designed offline but will require real test data to refine and ensure their completeness.

In order to link together the safety requirements and the verification specification, this paper begins the development of a safety case using Goal Structured Notation (GSN) [7] by introducing a GSN pattern [8, 9] that can be used to argue safe avoidance. This provides a methodology for linking evidence about system design and operation through to high level safety requirements which play a crucial role in developing the argument that would allow ROBO-GUIDE to be deployed in its intended environment. This approach taken will identify a collection of possible hazardous states, centred around ROBO-GUIDE being a trip hazard. By analysing the possible states a design for the implementation of movement will be deduced which will mitigate the risks. This will be presented as a GSN pattern linking the safety goals using evidence derived from the verification of the individual components which will build into the overall safety case so that ROBO-GUIDE could be deployed.

In the remainder of this paper we develop the safety case using methods appropriate to GSN: section 2 describes the robot that will be deployed as ROBO-GUIDE including constraints on operating conditions in the expected environment; section 3 presents an initial collection of risks present in the operation of ROBO-GUIDE within the set environment; section 4 builds a collection of operational states to help mitigate these risks; section 5 discusses verification techniques; section 6 discusses the demonstration of the safety of ROBO-GUIDE within the expected operating environment; and section 7 draws conclusions from this work and identifies the path for future research.

2 The Robot

The robot used as the development platform for ROBO-GUIDE will be the Pioneer LX, from Adapt MobileRobots, shown in Figure 1. This is a wheeled robot, capable of operating for up to 13 hours before requiring recharging, which can be accomplished autonomously using a charging station provided in a known location. The Pioneer LX has front and rear ultrasonic sensors, and a laser scanner, which can be used to identify and avoid potential obstacles. It also has a front bumper that can be used to trigger a halt condition, when contact with an object is detected.

2.1 Operating Limitations and Specifications

The Pioneer LX User Guide provides some general limitations on both the operating environment and safe operation. Environmental limitations include avoiding:

- glass doors and walls
- pits without railings or low bumpers
- floors with access panels removed

Fig. 1. The Pioneer LX

– loose cables, hoses, etc...
– large, highly-reflective objects

Additional, operations should be limited to

– slopes of $< 1:12$
– steps of $< 15mm$
– gaps of $< 15mm$
– temperatures between $5 - 40^oC$
– humidity between $5 - 95\%$, non-condensing

All of these limitations are satisfied by the environment in which the Pioneer LX will be operated, therefore no additional mitigation is needed.

To ensure safe operation, it is not permitted to:

– ride the robot
– exceed a $60kg$ payload
– operate with a fouled drivetrain

As the Pioneer LX is to be operated in proximity to possibly uncooperative humans, it is possible that these safety restrictions could be breached. To ensure safe operation is maintained the robot must act accordingly in these situations; this behaviour is discussed in the following sections.

3 Trip Hazard Analysis and Risk Assessment

Initial hazard analysis of ROBO-GUIDE reveals a collection of risk areas. Whilst these areas initially seem limited, the operational environment of ROBO-GUIDE produces a series of complex scenarios that require careful management in order to produce a convincing safety case.

The Pioneer LX is only 45cm tall, and presents a trip hazard. However, the nature of the operation of the ROBO-GUIDE brings it into contact with a variety of environmental states that can promote this risk, which can be analysed using this collection of states [2].

Any situation where the ROBO-GUIDE is brought into close contact with humans will give rise to a trip hazard. Although the Pioneer LX uses a laser scanner for object avoidance there are a collection of scenarios that can still present where a trip hazard is present. Whenever the ROBO-GUIDE is stopped within the building it prevents a stationary trip hazard. There are three possible sets of conditions when ROBO-GUIDE will stop during normal operation:

H1 When the laser scanner detects an obstacle whilst moving through an area it expects to be clear (for example a person walking in its way), the Pioneer LX will stop. As soon as it stops, due to its height, it will become a trip hazard.

H2 ROBO-GUIDE will naturally come to a halt in populated areas during much of its operational life, for example when waiting for the lift, in the lift itself, or behind a door. In all of these cases ROBO-GUIDE will be entering a higher-risk state, where it is a stationary trip hazard. However, it cannot proceed as a fixed-object is blocking progress.

H3 Whenever the Pioneer LX encounters a person in its path, it will stop if it cannot find a path to go around. It is, therefore, very easy to manipulate this behaviour so that ROBO-GUIDE can be made to stop in a dangerous position, for example in front of the door to an office.

When ROBO-GUIDE detects a human obstacle (case 1) it should make anyone nearby aware of its position through an audible warning. If it detects a fixed piece of the environment (case 2), whilst waiting for a door to open, it should wait in a pre-determined safe area which can be identified, a-priori, through analysis of the map - still proving an audible warning of its presence.

In case 3, malicious behaviour can place the robot in a dangerous position. Like case 1, ROBO-GUIDE should broadcast its presence. However, it should be continually aware of the location within which it has stopped. Therefore, ROBO-GUIDE can take immediate action to vacate the area as quickly as possible, and relocate to a local safe zone with the same behaviour as case 2.

4 Operational States

There are a collection of operational states that can be used to define operation of the Pioneer LX as a ROBO-GUIDE. These states capture the need to maintain

safe operation within a crowded environment, to be as unobtrusive as possible, and to limit potential hazards:

- Temporary Park (out of lift) - entered when ROBO-GUIDE may be in a hazardous position whilst it is waiting for the lift, waiting at a door or, detecting an obstacle. This is a time-limited state that enables the robot to enter the lift, or pass through a door. In these positions it may prove to be a trip hazard, therefore this is necessarily a temporary state. This should be linked in to providing information to members of the public nearby, and is potentially an interesting state in which to investigate human-robot interaction.
- Temporary Park (in lift) - entered when ROBO-GUIDE is in the lift. When in this state the robot will be changing floors.
- Permanent Park - entered when the ROBO-GUIDE is parked in a safe position on the map. This should be out of the way of common public thoroughfares, to prevent causing a trip hazard.
- Charging - entered when ROBO-GUIDE has returned to its charging station.
- Moving (clear) - entered when the ROBO-GUIDE is moving within the map and away from locations such as doors.
- Moving (hazard) - when ROBO-GUIDE moves into the vicinity of a door, such as an office door or entrance, it will become a temporary hazard until it leaves the area. Should a breakdown occur within this area ROBO-GUIDE will enter the Error (serious) state, as it presents an immediate hazard and must be recovered quickly.
- Error (serious) - entered when ROBO-GUIDE encounters an error condition from a hazardous state or within a corridor. This causes an alarm to be sent to main robot control station indicating its position and a description of the error that has occurred. This could be caused by several reasons, but is most likely to appear when the robot is unable to move whilst in a common thoroughfare or hazardous situation.
- Error (minor) - entered when ROBO-GUIDE encounters a failure from Permanent Park, potentially to indicate initialisation failure or a problem when charging.

The hazards defined within Section 3 can be directly linked to the operational states defined in this section through a series of scenarios define in Table 1. Identifying the states limits the hazards to a smaller potential subset, which can then be further targeted for mitigation. Because of the size of the Pioneer LX, at 45cm, it will always prove a trip hazard and the conditions within which they can arrive should be detailed, these are a collection of effective state combinations of the robot within the environment and ROBO-GUIDE itself. The combinations of these states forms the potential for hazards and should reflect in mitigation which can then be verified.

Hazard	Operational State	Description
H1	Moving (clear) & Moving (hazard)	Whenever ROBO-GUIDE is moving within the corridor it will present a tip hazard to anyone in that corridor whether it is travelling or stopped.
H1	Moving (clear) & Moving (hazard)	Whenever ROBO-GUIDE is moving within the corridor it will present a tip hazard to anyone in that corridor any failure of the sensors providing sense and avoid will present an extra trip hazard.
H2	Temporary Park (in lift)	Whenever ROBO-GUIDE is in the lift it will pose a trip hazard to other users. Additionally in a crowded lift, its low height (45cm) will pose an additional problem as anyone entering may not be aware that ROBO-GUIDE is in the lift.
H2	Temporary Park (out of lift) & Moving (hazard)	When waiting for the lift ROBO-GUIDE will be parked in the corridor, acting as a trip hazard waiting for the lift to arrive.
H2	Temporary Park (out of lift) & Moving (hazard)	When waiting for a door to be opened ROBO-GUIDE will be parked in the corridor, acting as a trip hazard waiting for the lift to arrive.
H3	Temporary Park (out of lift) & Moving (hazard)	If a person stands in front of the ROBO-GUIDE then it will stop. Therefore ROBO-GUIDE can be made, potentially maliciously, to stop in front of an office door and can then present a trip hazard to whoever exits the room.
H3	Error (serious)	If a person attempts to ride the Pioneer LX then ROBO-GUIDE it will stop as riding may damage the robot. Therefore ROBO-GUIDE can be made to stop in front of an office door and can then present a trip hazard to whoever exits the room.
H3	Error (serious)	Any failure on the Pioneer LX will cause it to cease movement, this means it will remain in position acting as a trip hazard in whatever its final position, in a corridor, behind a door or waiting for the lift.

Table 1. Linking Operational States to Hazards

5 Verification

Before ROBO-GUIDE can be safely deployed in a building populated with a large number of unsuspecting people it is important that its operation be verified against a set of specifications. These specifications can be derived from a number of sources, such as the operational limitations and states defined in Sections 2.1 and 4 respectively. Specifications derived in this way will concern the safe operation of ROBO-GUIDE in an uncertain environment. Additional specifications can be derived from the requirement that ROBO-GUIDE successfully performs its task.

It is important to consider performance specifications in addition to those for safety, otherwise the robot may not behave as desired. For example, a robot which immediately parks in the corner of a room may be considered perfectly safe (i.e. it poses no hazard to humans), but in doing so it will never achieve its goal[1]. These two forms of specification are discussed in the following sections.

5.1 Safety Specification

The operational limitations and states of ROBO-GUIDE are conditioned on the state of the environment. The definition of the environmental conditions for each state is written in terms of abstractions such as *in the vicinity of a door* and *in a safe position*. Therefore ROBO-GUIDE requires an abstraction engine [4] to translate its continuous state (e.g. (x, y) position on a map) in to a set of discrete abstractions.

With the discrete abstractions defined in this way it is possible to use formal verification methods to prove that the decision making logic of ROBO-GUIDE will always adhere to a particular specification. Examples of a safety based specification include:

- ROBO-GUIDE should never enter the *Moving (clear)* or *Moving (hazard)* states if it believes *someone is riding it*
- ROBO-GUIDE should never enter the *Permanent Park* state when not *in a safe position*
- If ROBO-GUIDE is *in the vicinity of a door* then at some point in the future it must enter the *Moving (hazard)* or the *Error (serious)* state
- If ROBO-GUIDE *encounters a failure* in any state it should transition to, and remain in, either *Error (serious)* or *Error (minor)*

5.2 Performance Specification

In addition to ensuring ROBO-GUIDE performs safely in the environment it is also important to know that it will complete its desired task successfully. One of the most challenging aspects of the task facing ROBO-GUIDE is the need to navigate a lift, with the help of unsuspecting humans. This challenge introduces additional specifications such as:

- If ROBO-GUIDE is *in the lift* it will, at some point in the future, be *on the correct floor*
- If ROBO-GUIDE is *in the lift* it will, at some point in the future, not be *in the lift*
- If ROBO-GUIDE is not *on the correct floor* it will, at some point in the future, be *in the lift*

It can be seen that these performance specifications include the additional discrete abstractions *in the lift* and *on the correct floor*. During the development

[1] With the exception of the fairly limited goal *park in the corner of the room*

of ROBO-GUIDE it is necessary to ensure that all the discrete states which are important to its safety or performance are determined and suitable specifications derived. It is likely that this process will require the operation of ROBO-GUIDE in a number of supervised tests to allow the refinement of the discrete abstractions and specifications.

6 Safety of Operation

The safety of operation of ROBO-GUIDE is paramount in allowing it to function without human supervision. In order for such a robot to be deployed in such a function a solid body of evidence must be produced that demonstrates why this is so. This section discusses how this evidence can be sourced and communicated.

6.1 Safety Cases

A safety case is a method for arguing, and providing the evidence, that a system is safely capable of operating within an environment [11], and to demonstrate how that safety has been achieved [10]. Producing such a argument is necessary to show that a system is capable of operating within a certain context or domain, whilst maintaining safe operation. For robots, especially those that come into contact with humans, the construction of the safety case is an important component in ensuring that concerns can be correctly addressed [6], and that mitigation can be undertaken during design [5, 14, 13].

Goal Structuring Notation (GSN) provides a method for outlining the safety case to argue, in a "clear, comprehensible and defensible manner" that a system is safe to operate in a given context [7]. It is implemented through a community standard set of available symbols [12] which comprise an argument.

A safety case is comprised of three key pieces of information:

- The requirements and objectives that are required to maintain safe operation.
- The evidence that shows how the safety of the operation has been considered.
- An argument that links the evidence collected to the safety requirements and objectives.

GSN presents the argument as a series of blocks. Each claim or "Goal" is broken down into sub-"Goals" which show how smaller, elemental, pieces of the overall "Goal" are supported. These sit in the overall environment that the system will be used in, denoted by the "Context" of operation. "Goals" are linked via the "Strategy" that is used to partition them, the technique that has been used to break the "Goals" down into smaller components. At the base sit "Solutions" which show the evidence for support, which can then be traced up through the structure. It is also important to record any "Assumptions" that are made about the operation of the system. Any strategy can be backed up by the "Justification" defining its use, for example calling out to an appropriate standard. If a "Goal" is to be considered later then it can have a diamond

shaped box attached which indicates that it is intentionally "Undeveloped" to be completed more fully at a later date.

The application to such a mobile robot is clear; if a robot is allowed to roam free within an open public building it will come into contact with users with a wide-ranging experience of robots. The safety case needs to argue about how the robot will operate safely in this environment, in spite of the influence of people. The verification plays a crucial role in showing the supporting evidence which can then be used to argue that the state structure is satisfactory to ensure the safety requirements can be met.

6.2 A Safety Case for ROBO-GUIDE

This section will define the argument structure for ROBO-GUIDE that can be used to record the safety considerations taken during the design phase, verification to ensure correct design and implementation, and record operational concerns. The top level claims for the safety of the robot, will gradually be broken down through a series of steps to link them to the verification steps identified in Section 5. Each step will be explained with the logic behind it so that transparency can be maintained.

Figure 2 shows a GSN fragment for arguing the safety of ROBO-GUIDE in its operational environment using version 1 of the GSN Standard [12]. This builds the argument based around the premises shown in Goal G1 that ROBO-GUIDE is safe to operate, in its natural operating environment (around humans who may, or may not be aware of its presence as defined by Context C1). By satisfying all of the hazards that are present within a Functional Hazard Analysis, as specified by Context C2, the system can be assured to be functionally safe within the set operating environment, Goal 2.

In order to satisfy Goal 2, Strategy 1 argues that all hazards have been found, under Assumption A1 that the Functional Hazard Analysis has been successful. In this paper only hazards associated with the movement of the robot have been considered. Therefore other hazards sit within Goal G6, marked Undeveloped, which requires further expansion but is out of scope for this paper.

Goal G6, covers other hazards of movement not associated with collision, such as the drive-train becoming fouled. This can be accomplished using extra sensors to detect fouling of the drive-train and verification to ensure that all motion is halted. However, one particular risk has been highlighted within the manual of the Pioneer LX, it cannot be ridden, and has a maximum carrying capacity of 60kg, highlighted in Section 2.1. In order to mitigate this risk, Solution Sn7 calls for a load cell to be added to the top surface of the Pioneer LX, and verification undertaken to ensure that ROBO-GUIDE will not progress whilst overloaded.

This paper has considered hazards caused by the movement of a Pioneer Lx deployed as a ROBO-GUIDE in a crowded environment. The three scenarios that present a particular problem are outlined in Section 3, and require mitigation in order to satisfy safe behaviour. A collection of states have been established to avoid these behaviours where possible, outlined in Section 4 as Hazards H1,

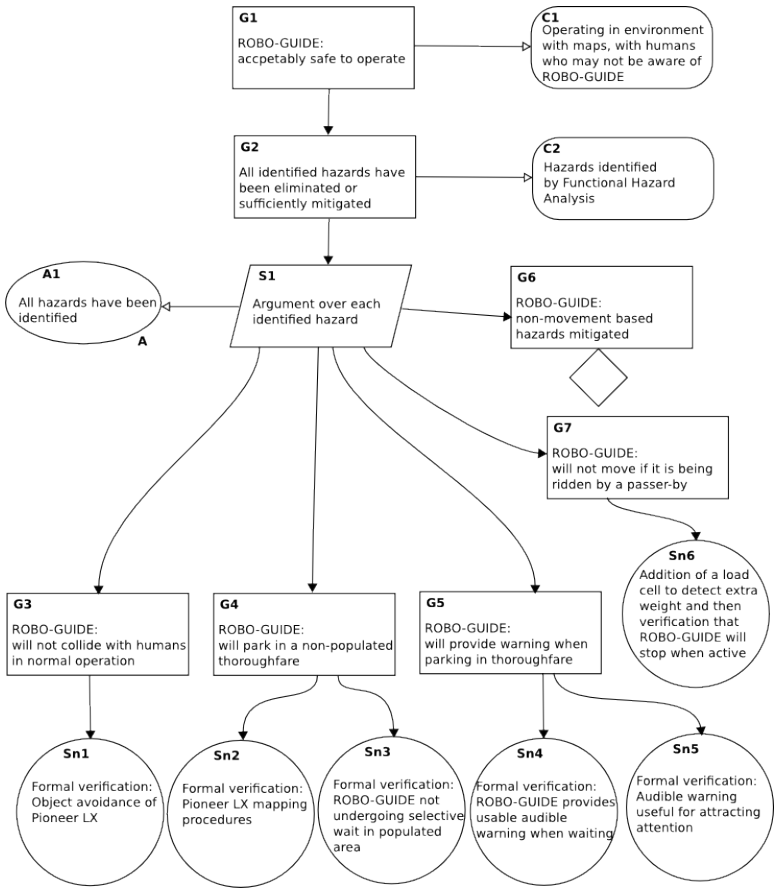

Fig. 2. GSN Fragment for ROBO-GUIDE using standard GSN Symbols defined in [12]

H2 and H3. Goal 3 reflects the need to avoid collision with humans under normal operation, Solution Sn1 presents information from verification techniques outlined in Section 5 to ensure that the onboard sensors will provide general collision detection, and the conditions under which this may not be so.

Goal G4 reflects the need of ROBO-GUIDE (when stopping) to park in a non-populated thoroughfare, so that it is out of the way of anybody passing through. This is achieved via Solutions Sn2 and Sn3, indicating that non-populated areas of the map are successfully identified (Sn2); including areas such as office doors, and ensuring that when ROBO-GUIDE undertakes a wait it will not halt in one of these whenever possible (Sn3). Goal G5 reflects the need of ROBO-GUIDE to provide an audible warning to passers-by, when it waits in a throughfare. This is satisfied by Solutions Sn5 and Sn6, which will be heavily influenced by the human-robot interaction components of the ROBO-GUIDE project [3].

A pattern is a GSN fragment that presents an argument that can be reused in different cases [8, 9]. This is useful when developing future arguments as they can naturally be slotted in to the structure. In this case the GSN fragment has been developed to show a robot that present a potential trip hazard whilst travelling autonomously around a building. The various combinations of cases that support safe operation have been considered so that the design is generic and so leads on to being able to deploy in different safety cases.

7 Conclusions and Future Work

This paper has outlined some potential hazards that a Pioneer LX may encounter when used as ROBO-GUIDE for leading members of the public around a set of office buildings. It has begun the process of identifying potential hazards associated with movement through the environment, and the need to keep clear of humans or alert them to its presence. To this end the initial stages of a safety case have been outlined using Goal Structured Notation to record these possible hazards and link them to mitigation strategies, such as permitted robot states, and verification techniques to show that these have been correctly implemented. This has produced a GSN pattern that can be used for a robot that is traversing a populated corridor.

This work presents the foundation of the safety and verification side of ROBO-GUIDE which is under development [1]. This work forms the basis to build a software specification which will ensure a justifiably safe robot, that can be allowed to move freely within a building.

References

1. Aitken, J.M., Boorman, L., Cameron, D., Chua, D., Collins, E., Fernando, S., Law, J., McAree, O., Martinez-Hernandez, U.: ROBO-GUIDE: towards safe, reliable, trustworthy, and natural behaviours in robotic assistants. In: Proceedings of Towards Autonomous Robotic Systems (TAROS) (submitted) (2015)
2. Aitken, J.M., Alexander, R., Kelly, T.: A risk modelling approach for a communicating system of systems. In: Proceedings of the 2011 IEEE International Systems Conference (SysCon). pp. 442–447 (2011)
3. Cameron, D., Collins, E., Chua, D., Fernando, S., McAree, O., Martinez-Hernandez, U., Aitken, J.M., Boorman, L., , Law, J.: Help! I cant reach the buttons: Facilitating helping behaviors towards robots. In: Proceedings of Living Machines (submitted) (2015)
4. Dennis, L.A., Fisher, M., Lincoln, N.K., Lisitsa, A., Veres, S.M.: Declarative abstractions for agent based hybrid control systems. In: Declarative Agent Languages and Technologies VIII, pp. 96–111. Springer (2011)
5. Do Hoang, Q.A., Guiochet, J., Powell, D., Kaaniche, M.: Human-robot interactions: Model-based risk analysis and safety case construction. In: 6th European Congress on Embedded Real-Time Software and Systems (2012)
6. Harper, C., Virk, G.: Towards the development of international safety standards for human robot interaction. International Journal of Social Robotics 2(3), 229–234 (2010)

7. Kelly, T., Weaver, R.: The goal structuring notation–a safety argument notation. Proceedings of the dependable systems and networks 2004 workshop on assurance cases (2004)
8. Kelly, T., McDermid, J.: Safety case construction and reuse using patterns. In: Daniel, P. (ed.) Safe Comp 97, pp. 55–69. Springer London (1997)
9. Kelly, T., McDermid, J.: Safety case patterns - reusing successful arguments. In: IEE Colloquium on Understanding Patterns and their Application to Systems Engineering (January 1998)
10. Menon, C., Hawkins, R., McDermid, J.: Defence standard 00-56 issue 4: Towards evidence-based safety standards. In: Dale, C., Anderson, T. (eds.) Safety-Critical Systems: Problems, Process and Practice, pp. 223–243. Springer London (2009)
11. MoD Interim Defence Standard: Standard 00-56 issue 4. Safety Management Requirements for Defence Systems (2007)
12. Origin Consulting Limited: GSN community standard version 1. Tech. rep. (2014)
13. Schmidt, D., Berns, K.: Risk and safety aspects for wall-climbing robots. In: ISR/Robotik 2014; 41st International Symposium on Robotics; Proceedings of. pp. 1–8. VDE (2014)
14. Täubig, H., Frese, U., Hertzberg, C., Lth, C., Mohr, S., Vorobev, E., Walter, D.: Guaranteeing functional safety: design for provability and computer-aided verification. Autonomous Robots 32(3), 303–331 (2012)